Acceptable and Unacceptable Use of State Provided Computer Resources

Computer resources are provided to assist staff in completing their job tasks. *However, incidental and occasional personal use is permitted, as long as such does not:*

- Interfere with existing rules or policies pertaining to the agency
- Disrupt or distract the conduct of state business(e.g. due to volume or frequency)
- Involve solicitation
- Involve a for-profit personal business activity
- Have the potential to harm the state
- Involve illegal activities

I recommend the telephone use standard. Supervisors allow occasional use of the telephone for personal use. However, if a employee is spending "a lot of time" on personal calls is making toll calls it is a problem. It is the same for use of the computer resources including using the Internet or printing personal documents. Don't spend "a lot of time" planning your next vacation, checking sports scores or the stock market. If you print personal documents on Agency printers expect to pay for the cost of paper and printing.

Unacceptable Use of IT Resources

The first and foremost rule for using these technologies is:
Don't say, do, write, or acquire anything that you wouldn't be proud to have everyone in the world learn about if the electronic records are laid bare. Any use of the state-provided IT resources for inappropriate purposes, or in support of such activities, is prohibited (unless authorized through job responsibilities). **The following list is currently considered unacceptable use of state-provided IT resources.**

1. **Illegal Use.** Any use of state-provided IT resources for illegal purposes, or in support of such activities. Illegal activities shall be defined as any violation of local, state or federal laws.
2. **Commercial use.** Any use for commercial purposes, product advertisements or "for profit" personal activity.
3. **Sexually explicit.** Any sexual explicit use, whether visual or textual. You shall not view, transmit, retrieve, save or print any electronic files which may be deemed as sexually explicit.
4. **Religious or Political Lobbying.** Any use for religious or political lobbying.
5. **Copyright Infringement.** Duplicating, transmitting, or using software not in compliance with software license agreements. Unauthorized use of copyrighted materials or another person's original writings. ***Installing software not owned or authorized by USOR.***
6. **Unnecessary Use of IT Resources.** Wasting IT resources by intentionally:
   - Placing a program in an endless loop
   - Printing unnecessary amounts of paper
   - Disrupting the use or performance of state-provided IT resources or any other computer system or network (for example, unauthorized world wide web pages, recurrent mass communications):
   - Storing any information or software on state-provided IT resources which are not authorized by the agency.
   - Use of "Instant messenger, streaming audio and video" and other network resource intensive non-work related programs.
7. **Security Violations.** Accessing accounts within or outside the state's computers and communications facilities for which you are not authorized or do not have a business need. Copying, disclosing, transferring, examining, renaming or changing information or programs belonging to another user unless you are given express permission to do so by the user responsible for the information or programs.
   Violating the privacy of individual users by reading Email or private communications unless you are specifically authorized to maintain and support the system. Representing yourself as someone else, fictional or real.
   Be responsible for the use of your accounts. **Under no condition should you give your password to another person.** Guard yourself against unauthorized access to your accounts:
   - Change your passwords with regular frequency or in accordance with the USOR policy regarding the frequency of changing passwords.
   - ***Do not use obvious passwords.***
8. **Viruses.** Knowing or inadvertently spreading computer viruses. "Computer viruses" are programs that can destroy valuable programs and data. To reduce the risk of spreading computer viruses, do not import files. Do not run e-mail attachments that have a **.exe** extension. All floppy disks must be

scanned prior to using them on any computer attached to USOR networks. **If you are unsure of the steps to scan a disk. Please contact your computer support staff for assistance.**

9. **Junk Mail.** Distributing "***junk***" mail, such as "***chain letters***", "***advertisements***" or "***unauthorized solicitations***".

10. **Confidential Information. Transmitting classified information under Government Records Access and Management Act without proper security.** The Internet provides the ability to communicate , collaborate with others and access information throughout the world**. Within the State GroupWise system email files are protected.** However, anything you transmit over the Internet is subject to interception, reading, and copying by other people.

11. **Privacy Issues and Legal Implications.** A state agency has the right to access the contents of electronic files as required for legal audit or legitimate state operational or management purposes (Administrative Rule R365-4, Information Technology Security). Do not transmit personal information about yourself or someone else using State applied IT resources without proper authorization. The confidentiality of such material cannot be guaranteed. Email and other electronic files may be accessible through the discovery process in the event of litigation. Each of these technologies may create a "record" and therefore are reproducible and subject to judicial use. In the course of their work, managers, network and computer operations personnel or system administrators may monitor the network and computer operations personnel or system administrators may monitor the network or email system (administrative Rule R365-4, Information Technology Security). It should be assumed that the content of files and email messages may be seen by these authorized individuals during the performance of their duties.

12. **Use of Email.** The GroupWise system allows us to block known viruses at the GroupWise gateway. However, if individuals are receiving external messages and email which do not go through this gateway a significant part of our anti-virus protection is rendered useless.
    - **It is prohibited to access any email account other than GroupWise on USOR networks. If you have email accounts on any other system (HotMail, Netscape, Yahoo, US West, etc) you may not access your external email while at work.**
    - **It is prohibited to install or use messaging software (AOL Instant messenger, Yahoo Messenger, etc.) on USOR networks.**
    - **It is prohibited to attach executable programs to internal GroupWise email. Simply do not attach a file to any GroupWise email except the following:**
        a. Word processing text documents (Word or WordPerfect) .doc or .wpd
        b. Spreadsheet files (Excel or Quattro Pro) .xls or .wb3
        c. Presentation files (Power Point or Presentations) .ppt or .shw

If you have a need to attach a file which is not listed above call and discuss the need with the computer support staff.